PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282805
(43)Date of publication of application : 15.10.1999

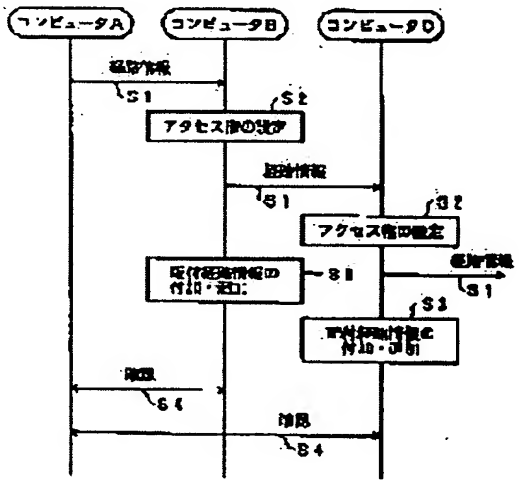
(51)Int.Cl. G06F 15/00
G06F 12/14
G06F 13/00

(21)Application number : 10-081454
(22)Date of filing : 27.03.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MORIHIRO SEIJI

(54) RESOURCE ACCESS CONTROL METHOD, SYSTEM THEREFOR AND STORAGE MEDIUM STORING RESOURCE ACCESS CONTROL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a resource access control method/system and a storage medium storing a resource control access program which prevents a specific manager from concentrating the grant and deprivation of access right to all jobs when the distribution of access right is desired in a wide range under a rational restriction, improves the giving efficiency of the access right and attains the effective auditing of distribution of access right and also the deprivation of the access right and the giving right of the access right by an access request method together with addition of the access right distribution path information.



SOLUTION: Path information S1 is transferred among computers A, B and C to show distribution paths which distribute the access right to these computers included in a computer network to access an object respectively. Meanwhile, the access right is set to the information S1 and the information S1 is given and added (S3) every time a distribution path list is transferred among the computer access control monitors. Then it's confirmed whether or not the access right is properly distributed based on the distribution path list.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－282805

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｄ
	12/14	３１０		12/14	３１０Ｋ
	13/00	３５１		13/00	３５１Ｚ

審査請求　未請求　請求項の数15　ＯＬ　（全 19 頁）

(21)出願番号　特願平10－81454

(22)出願日　平成10年(1998) 3月27日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号

(72)発明者　森廣　政治
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

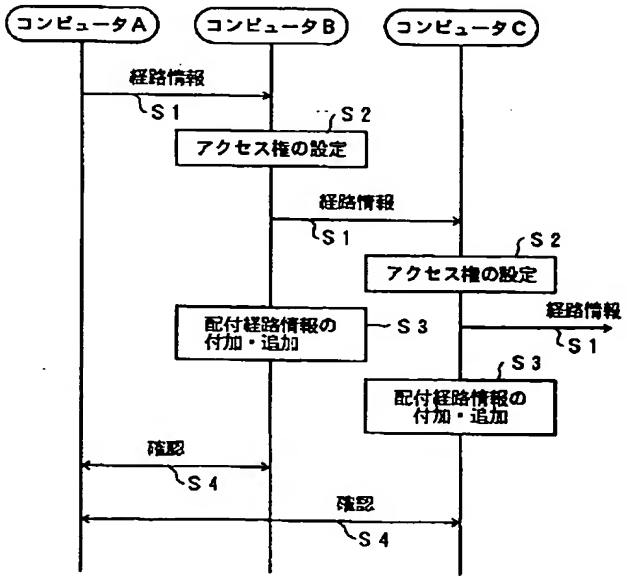
(54)【発明の名称】　資源アクセス制御方法及びシステム及び資源アクセス制御プログラムを格納した記憶媒体

(57)【要約】

【課題】　合理的な制限下で広範囲にアクセス権限を配布したい場合でのアクセス権限の付与や剥奪を特定の管理者が全作業を集中させず、アクセス権限の付与効率を向上すると同時に、アクセス権配布経路情報を伴い、アクセス要求する手法にによりアクセス権配布の効率的監査、アクセス権の剥奪及びアクセス権の付与権の剥奪を可能とする資源アクセス制御方法及びシステム及び資源アクセス制御プログラムを格納した記憶媒体を提供する。

【解決手段】　本発明は、対象をアクセスするためのアクセス権をコンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報を該コンピュータ間において授受すると共に、該経路情報へのアクセスの権を設定し、コンピュータのアクセス制御モニタ間で配布経路リストの授受を行う毎に、配布経路情報の付与及び追加を行い、配布経路リストによりアクセス権の配布行為が適切に行われたかを確認する。

本発明の原理を説明するための図



【特許請求の範囲】

【請求項１】　単独のコンピュータもしくは、複数のコンピュータを通信回線で接続したコンピュータネットワーク上において、該コンピュータに蓄積された情報などの資源（以下、対象と記す）を定められた規則に基づいて利用者（以下、主体と記す）の利用を制限する資源アクセス制御方法において、
前記対象をアクセスするためのアクセス権を前記コンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報にアクセス権を設定して、該経路情報を該コンピュータ間、または、単独のコンピュータ内において授受し、
前記コンピュータのアクセス制御モニタ間で前記経路情報の授受を行う毎に、配布経路情報の付与及び追加を行い、
前記経路情報によりアクセス権の配布行為が適切に行われたかを確認することを特徴とする資源アクセス制御方法。

【請求項２】　配布アクセス権に対応する対象を有する主体から複数のコンピュータを経由して、前記経路情報が配布されると、
配布されたコンピュータＡでは、前記経路情報に配布経路情報を追加し、アクセス制御情報を更新し、該経路情報をコンピュータＢに配布し、
前記コンピュータＢでは、前記経路情報に配布経路情報を追加し、アクセス制御情報を更新し、
前記経路情報を配布する処理を、配布するコンピュータ数分繰り返して、該経路情報を配布する請求項１記載の資源アクセス制御方法。

【請求項３】　前記アクセス権の配布行為を確認する際に、
前記経路情報の配布元のコンピュータから、配布先のコンピュータに対して、経路情報の有無、経路情報へのアクセス権の確認を行い、
確認結果に基づいてアクセスの可否判断を行う請求項１記載の資源アクセス制御方法。

【請求項４】　前記経路情報の配布元のコンピュータにおいて、該経路情報の配布を行おうとしているコンピュータに配布の許諾を行い、
許諾した場合に、アクセス権限配布管理リストに登録し、
アクセス要求を行っている主体が前記アクセス権限配布管理リストに登録されている場合に、アクセスを許可する請求項１記載の資源アクセス制御方法。

【請求項５】　前記アクセス権限配布管理リストから任意の主体を削除することによりアクセス拒否を行う請求項４記載の資源アクセス制御方法。

【請求項６】　単独のコンピュータもしくは、複数のコンピュータを通信回線で接続したコンピュータネットワークにおいて、該コンピュータに蓄積された情報などの資源（以下、対象と記す）を定められた規則に基づいて利用者（以下、主体と記す）の利用を制限する資源アクセス制御システムであって、
前記コンピュータは、
前記対象をアクセスするためのアクセス権を前記コンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報と、
前記経路情報へのアクセスの権を設定するアクセス権設定手段と、
前記経路情報を該コンピュータ間において授受する経路情報配布手段と、
前記コンピュータのアクセス制御モニタ間で前記経路情報の授受を行う毎に、前記経路情報に配布経路情報の付与及び追加を行う更新手段と、
前記経路情報によりアクセス権の配布行為が適切に行われたかを確認する確認手段とを有することを特徴とする資源アクセス制御システム。

【請求項７】　前記経路情報配布手段は、
配布アクセス権に対応する対象を有する主体から少なくとも１つのコンピュータを経由して、前記経路情報が配布されたコンピュータにおいて、前記経路情報に配布経路情報を追加し、アクセス制御情報を更新し、該経路情報を他のコンピュータに配布する処理を、配布するコンピュータ数分繰り返す手段を含む請求項６記載の資源アクセス制御システム。

【請求項８】　前記確認手段は、
前記経路情報の配布元のコンピュータから、配布先のコンピュータに対して、経路情報の有無、経路情報へのアクセス権の確認を行うアクセス権確認手段と、
前記アクセス権確認手段の確認結果に基づいてアクセスの可否判断を行う判定手段を含む請求項６記載の資源アクセス制御システム。

【請求項９】　前記経路情報の配布を行おうとしているコンピュータに配布の許諾を行う配布許諾手段と、
前記配布許諾手段において、許諾した場合に、アクセス権限配布管理リストに登録するリスト登録手段と、
アクセス要求を行っている主体が前記アクセス権限配布管理リストに登録されている場合に、アクセスを許可するアクセス許可判定手段とを更に有する請求項６記載の資源アクセス制御システム。

【請求項１０】　前記アクセス権限配布管理リストから任意の主体を削除することによりアクセス拒否を行うアクセス権剥奪手段を更に有する請求項９記載の資源アクセス制御システム。

【請求項１１】　単独のコンピュータもしくは、複数のコンピュータを通信回線で接続したコンピュータネットワークにおいて、該コンピュータに蓄積された情報などの資源（以下、対象と記す）を定められた規則に基づいて利用者（以下、主体と記す）の利用を制限する資源アクセス制御システムにおけるコンピュータに搭載される

資源アクセス制御プログラムを格納した記憶媒体であって、
前記対象をアクセスするためのアクセス権を前記コンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報へのアクセスの権を設定するアクセス権設定プロセスと、
前記経路情報を他のコンピュータに配布する経路情報配布プロセスと、
前記経路情報配布プロセスが起動される毎に、前記経路情報に配布経路情報の付与及び追加を行う更新プロセスと、
前記経路情報によりアクセス権の配布行為が適切に行われたかを確認する確認プロセスとを有することを特徴とする資源アクセス制御プログラムを格納した記憶媒体。
【請求項１２】　前記経路情報配布プロセスは、
配布アクセス権に対応する対象を有する主体から少なくとも１つのコンピュータを経由して、前記経路情報が配布されたコンピュータにおいて、前記経路情報に配布経路情報を追加し、アクセス制御情報を更新し、該経路情報を配布する処理を、配布するコンピュータ数分繰り返すプロセスを含む請求項１１記載の資源アクセス制御プログラムを格納した記憶媒体。
【請求項１３】　前記確認プロセスは、
前記経路情報の配布先のコンピュータに対して、経路情報の有無、経路情報へのアクセス権の確認を行うアクセス権確認プロセスと、
前記アクセス権確認プロセスの確認結果に基づいてアクセスの可否判断を行う判定プロセスを含む請求項１１記載の資源アクセス制御プログラムを格納した記憶媒体。
【請求項１４】　前記経路情報の配布を行おうとしているコンピュータに配布の許諾を行う配布許諾プロセスと、
前記配布許諾プロセスにおいて、許諾した場合に、アクセス権限配布管理リストに登録するリスト登録プロセスと、
アクセス要求を行っている主体が前記アクセス権限配布管理リストに登録されている場合に、アクセスを許可するアクセス許可判定プロセスとを更に有する請求項１１記載の資源アクセス制御プログラムを格納した記憶媒体。
【請求項１５】　前記アクセス権限配布管理リストから任意の主体を削除することによりアクセス拒否を行うアクセス権剥奪プロセスを更に有する請求項１４記載の資源アクセス制御プログラムを格納した記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、資源アクセス制御方法及びシステム及び資源アクセス制御プログラムを格納した記憶媒体に係り、特に、コンピュータに蓄積された情報などの資源の利用を制限する資源アクセス制御方法及びシステム及び資源アクセス制御プログラムを格納した記憶媒体に関する。
【０００２】
【従来の技術】コンピュータに蓄積された情報などの資源の利用におけるアクセス制御は、図９に示すように、情報などの資源を利用する利用者（主体）と、利用される情報などの資源（対象）の関係をマトリクス状に表現したアクセス制御マトリクスの情報に基づいて、個々の利用をアクセス制御モニタ（あるいは、セキュリティ核とも言う）により表現するモデルにより、一般的に定式化される。
【０００３】このモデルに基づいて、従来実現されてきた方式として、図１０に示す第１の方式のように、アクセスマトリクスの有効要素のみを主体、対象、アクセス権の三つの組で構成する三つ組表で表現し、それに基づいてアクセス制御モニタにより実現する方式がある。さらに、図１１に示す第２の方式のように、図１０に示す方式における三つ組表の要素を主体毎に分類し、個々の主体毎の要素（資格あるいは、ケーパビリティと称す）の集合に対してカタログ概念を定義し、各々のカタログに含まれる資格（対象へのアクセス権）に基づいて、アクセス制御モニタにより実現する方式がある。
【０００４】また、図１２に示すように、図１１に示す第２の方式とは逆に、主体ではなく対象で、図１０に示す第１の方式により三つ組表の要素を分類し、個々の対象毎の要素の集合に対してアクセス制御リストという概念を定義し、対象毎に配置された該アクセス制御リストに基づいて、アクセス制御モニタにより実現する第３の方式がある。
【０００５】また、アクセス権の配布を可能とするために、図９のモデルに従い静的なアクセス制御マトリクスによる機能は維持するが、主体とアクセス制御マトリクス或いは、対象とアクセス制御マトリクス間の関係を動的に対応付け、その対応付けの変化でアクセス権の配布を実現する方式と、図１３に示すようなアクセス制御マトリクス自体へのアクセスを考慮に入れたアクセス制御モデルに従い、アクセス権の付与というアクセス制御マトリクスに対する更新権を用いることにより実現する方式が考えられている。
【０００６】図９に従った方式として、図１４に示すように、第１の方式における三つ組表の要素を分類し、個々の対象毎の要素の集合に対してアクセス制御リストという概念を定義し、対象側に付随して配置する第３の方式に、各々の主体を分類した第３の方式での資格の概念を導入した第４の方式がある。当該第４の方式では、資格の識別に公開鍵などの識別鍵情報を用いて、資格の認証をアクセス制御モニタから分離し、識別鍵情報の有無により判定するため、識別鍵情報を配布することにより、アクセス権の配布を可能にする方式である。この方式では、アクセス権をもつ全ての主体がアクセス権の付

与権も同時に持つことになる。

【０００７】図１３のモデルに従う方式としては、図９におけるアクセス制御マトリクスに相当する情報を図１５に示すようなリストなどの構造で保持し、アクセス権限の配布の前後関係を保持する第５の方式がある。この方式において、主体（サブジェクト）Ｓ－ａ、Ｓ－ｂ、Ｓ－ｃは、対象所有者から直接アクセス権を付与され、主体Ｓ－ｄ、Ｓ－ｅは、主体Ｓ－ａからアクセス権を付与され、主体Ｓ－ｆ、Ｓ－ｇは、主体Ｓ－ｂからアクセス権を付与され、主体Ｓ－ｈ、Ｓ－ｉは主体Ｓ－ｄからアクセス権を付与された状態を示している。この例の場合、アクセス権を配布した主体が、当該主体によりアクセス権を付与された被配布者の権限を変更可能とする制限を課することにより、アクセス権配布の系列の前の者（配布者）が後ろの者（被配布者）のアクセス権の変更を直接あるいは、関節に変更することを可能とし、かつ、アクセス権配布の系列の後ろの者が前の者のアクセス権の変更を不可とする。

【０００８】また、図１６に示すように、情報の構造は、第５の方式と同等であるが、第５の方式のようなアクセス権の配布者、被配布者による互いのアクセス権の変更に対する制限を課されず、権限の配布の系列に関係なく同等の権限を得る第６の方式がある。この第６の方式において、アクセス権の配布の関係は第５の方式と同じく、主体Ｓ－Ａ、Ｂ、Ｃは対象所有者から直接アクセス権を付与され、主体Ｓ－Ｄ、Ｓ－Ｅは、主体Ｓ－Ａからアクセス権を付与され、主体Ｓ－Ｆ、Ｓ－Ｇは、主体Ｓ－Ｂからアクセス権を付与され、主体Ｓ－Ｈ、Ｓ－Ｉは、主体Ｓ－Ｄからアクセス権を付与された状態を示している。しかし、各々の主体に対するアクセス権情報がリンクされている位置に関係なく、リンク上に現れる全ての主体のアクセス権情報を任意に変更／剥奪可能とすることにより、アクセス権の配布の系列を保持しないアクセス制御情報の実現が可能である。

【０００９】

【発明が解決しようとする課題】しかしながら、上記の第１、第２、第３の方式のいずれも、図９のモデルにあるように、主体と対象の必要な組み合わせに対して、アクセス権の静的な状態を与えることにより実現するため、この関係を最新状態に維持する作業が必要となる。ここで、主体や対象が単独のシステム上の要素など、限られた範囲に閉じている場合は問題ないが、複数の独立したシステムが相互に関連する状況では、アクセス権を付与する範囲が増大する。即ち、アクセス制御マトリクス相当の情報更新作業が増大する。このような環境で合理的な制限下で広範囲にアクセス権限を配布したい場合、適切な条件のもとにアクセス権を配布可能とする必要がある。また、アクセス権を配布可能とした場合、対象管理元が配布行為を最終的に掌握する意味で、配布により得たアクセス権に基づくアクセスに対して、関係する配布行為が適切に行われているが監査可能とし、また、監査結果に問題があった場合には適当な範囲で過去の配布されたアクセス権を剥奪可能とする必要がある。

【００１０】また、第４の方式のように、対象へのアクセス鍵を単純に提供するだけでは、一度アクセス権を配布された者を排除する場合には、鍵を変更して排除されるべき主体以外のアクセス権限取得者に変更を通知するか、対象管理元が主体毎に異なるアクセス鍵を用意するかのどちらかを実施する必要があり、何れにせよ対象管理元の負荷軽減の解決の上で問題が残る。

【００１１】第５の方式では、アクセス権の配布に制限はないため、系列上に同じ主体が存在する場合がある。具体的には図１６に示す主体Ｓ－４と主体Ｓ－６が同じ主体という状態も可能である。当該主体のアクセス権の有無という観点のみでは、このような重複したエントリが存在する状態も問題ないが、各々のアクセスの基盤となるアクセス権の付与経緯が判別できない当該方式では、どういう経緯で付与された権限をもってアクセスしたか等を監査する観点で問題がある。

【００１２】第６の方式では、第５の方式と同等の問題がある上、アクセス監査を考えると、個々の変更履歴を別途ログなどとして管理する必要があり、監査機能の実現で問題がある。本発明は、上記の点に鑑みなされたもので、アクセス権の変更に際してアクセス制御マトリクスあるいは、それに準じる制御情報を直接更新する従来の方式において困難であったアクセス権及びアクセス権の付与権の配布を容易に可能とすることにより、合理的な制限下で広範囲にアクセス権限を配布したい場合でのアクセス権限の付与や剥奪を特定の管理者が全作業を集中させず、アクセス権限の付与効率を向上すると同時に、アクセス権配布経路情報を伴い、アクセス要求する手法にによりアクセス権配布の効率的監査、アクセス権の剥奪及びアクセス権の付与権の剥奪を可能とする資源アクセス制御方法及びシステム及び資源アクセス制御プログラムを格納した記憶媒体を提供することを特徴とする。

【００１３】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。本発明（請求項１）は、単独のコンピュータもしくは、複数のコンピュータを通信回線で接続したコンピュータネットワーク上において、該コンピュータに蓄積された情報などの資源（以下、対象と記す）を定められた規則に基づいて利用者（以下、主体と記す）の利用を制限する資源アクセス制御方法において、対象をアクセスするためのアクセス権をコンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報にアクセス権を設定して、該経路情報を該コンピュータ間または、単独のコンピュータ内において授受し、コンピュータのアクセス制御モニタ間で経路情報の授受を行う毎に、配布経

路情報の付与及び追加を行い、経路情報によりアクセス権の配布行為が適切に行われたかを確認する。

【００１４】本発明（請求項２）は、配布アクセス権に対応する対象を有する主体から複数のコンピュータを経由して、経路情報が配布されると、配布されたコンピュータＡでは、経路情報に配布経路情報を追加し、アクセス制御情報を更新し、該経路情報をコンピュータＢに配布し、コンピュータＢでは、経路情報に配布経路情報を追加し、アクセス制御情報を更新し、経路情報を配布する処理を、配布するコンピュータ数分繰り返して、該経路情報を配布する。

【００１５】本発明（請求項３）は、アクセス権の配布行為を確認する際に、経路情報の配布元のコンピュータから、配布先のコンピュータに対して、経路情報の有無、経路情報へのアクセス権の確認を行い、確認結果に基づいてアクセスの可否判断を行う。本発明（請求項４）は、経路情報の配布元のコンピュータにおいて、該経路情報の配布を行おうとしているコンピュータに配布の許諾を行い、許諾した場合に、アクセス権限配布管理リストに登録し、アクセス要求を行っている主体がアクセス権限配布管理リストに登録されている場合に、アクセスを許可する。

【００１６】本発明（請求項５）は、アクセス権限配布管理リストから任意の主体を削除することによりアクセス拒否を行う。図２は、本発明の原理構成図である。本発明（請求項６）は、単独のコンピュータもしくは、複数のコンピュータを通信回線で接続したコンピュータネットワークにおいて、該コンピュータに蓄積された情報などの資源（以下、対象と記す）を定められた規則に基づいて利用者（以下、主体と記す）の利用を制限する資源アクセス制御システムであって、コンピュータは、対象をアクセスするためのアクセス権をコンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報１０と、経路情報１０へのアクセスの権を設定するアクセス権設定手段と、経路情報１０を該コンピュータ間において授受する経路情報配布手段２０と、コンピュータのアクセス制御モニタ間で経路情報の授受を行う毎に、経路情報に配布経路情報の付与及び追加を行う更新手段４０と、経路情報１０によりアクセス権の配布行為が適切に行われたかを確認する確認手段５０とを有する。

【００１７】本発明（請求項７）は、経路情報配布手段２０において、配布アクセス権に対応する対象を有する主体から少なくとも１つのコンピュータを経由して、経路情報が配布されたコンピュータにおいて、経路情報に配布経路情報を追加し、アクセス制御情報を更新し、該経路情報を他のコンピュータに配布する処理を、配布するコンピュータ数分繰り返す手段を含む。

【００１８】本発明（請求項８）は、確認手段５０において、経路情報１０の配布元のコンピュータから、配布先のコンピュータに対して、経路情報１０の有無、経路情報１０へのアクセス権の確認を行うアクセス権確認手段と、アクセス権確認手段の確認結果に基づいてアクセスの可否判断を行う判定手段を含む。

【００１９】本発明（請求項９）は、経路情報の配布を行おうとしているコンピュータに配布の許諾を行う配布許諾手段と、配布許諾手段において、許諾した場合に、アクセス権限配布管理リストに登録するリスト登録手段と、アクセス要求を行っている主体がアクセス権限配布管理リストに登録されている場合に、アクセスを許可するアクセス許可判定手段とを更に有する。

【００２０】本発明（請求項１０）は、アクセス権限配布管理リストから任意の主体を削除することによりアクセス拒否を行うアクセス権剥奪手段を更に有する。本発明（請求項１１）は、単独のコンピュータもしくは、複数のコンピュータを通信回線で接続したコンピュータネットワークにおいて、該コンピュータに蓄積された情報などの資源（以下、対象と記す）を定められた規則に基づいて利用者（以下、主体と記す）の利用を制限する資源アクセス制御システムにおけるコンピュータに搭載される資源アクセス制御プログラムを格納した記憶媒体であって、対象をアクセスするためのアクセス権をコンピュータネットワーク上のコンピュータに対して配布するアクセス権の配布経路を表現した経路情報へのアクセスの権を設定するアクセス権設定プロセスと、経路情報を他のコンピュータに配布する経路情報配布プロセスと、経路情報配布プロセスが起動される毎に、経路情報に配布経路情報の付与及び追加を行う更新プロセスと、経路情報によりアクセス権の配布行為が適切に行われたかを確認する確認プロセスとを有する。

【００２１】本発明（請求項１２）は、経路情報配布プロセスにおいて、配布アクセス権に対応する対象を有する主体から少なくとも１つのコンピュータを経由して、経路情報が配布されたコンピュータにおいて、経路情報に配布経路情報を追加し、アクセス制御情報を更新し、該経路情報を配布する処理を、配布するコンピュータ数分繰り返すプロセスを含む。

【００２２】本発明（請求項１３）は、確認プロセスにおいて、経路情報の配布先のコンピュータに対して、経路情報の有無、経路情報へのアクセス権の確認を行うアクセス権確認プロセスと、アクセス権確認プロセスの確認結果に基づいてアクセスの可否判断を行う判定プロセスを含む。

【００２３】本発明（請求項１４）は、経路情報の配布を行おうとしているコンピュータに配布の許諾を行う配布許諾プロセスと、配布許諾プロセスにおいて、許諾した場合に、アクセス権限配布管理リストに登録するリスト登録プロセスと、アクセス要求を行っている主体がアクセス権限配布管理リストに登録されている場合に、アクセスを許可するアクセス許可判定プロセスとを更に有

する。

【００２４】本発明（請求項１５）は、アクセス権限配布管理リストから任意の主体を削除することによりアクセス拒否を行うアクセス権剥奪プロセスを更に有する。上記のように、本発明は、アクセス権の配布をアクセス制御マトリクスの直接的変更ではなく、アクセス権の配布経路を表現した経路情報の授受と、当該情報へのアクセス権の設定と、アクセス制御モニタ間での経路情報授受の確認プロトコルで実現することにより、効率的なアクセス権の配布とその監査とを可能とする。

【００２５】

【発明の実施の形態】以下の説明に先立って、コンピュータに蓄積されたアクセス対象となる情報資源を以下では、「対象」と記し、当該対象をアクセスする利用者を「主体」として説明する。図３は、本発明の資源アクセス制御システムの構成図（その１）である。

【００２６】同図において、配布経路情報の配布にあたり、当該配布経路情報の配送元である主体Ａに関係する装置（コンピュータＡ）と、当該配布経路情報の配送先である主体Ｂに関係する装置（コンピュータＢ）とし、説明の簡単化のためにその構成を異にしているが、本来は、どのコンピュータについても同様の構成要素を有する。

【００２７】コンピュータＡは、対象１０１、対象識別部１０２、アクセス制御情報保持部１０３、アクセス制御部１０４、配布経路情報蓄積部１０５、対象アクセス部１１１、配布経路情報配布部１２０、及び主体識別部１９０より構成される。コンピュータＢは、対象２０１、対象識別部２０２、アクセス制御情報保持部２０３、アクセス制御部２０４、アクセス要求部２０７、対象アクセス部２１１、及び配布経路情報取得部２２０から構成される。

【００２８】主体識別部１９０、２９０は、主体を一意に識別する。対象識別部１０２、２０２は、対象１０１、２０１を一意に識別する。アクセス制御情報保持部１０３、２０３は、個々の対象１０１、２０１の個々の主体に対するアクセス制限情報を保持する。アクセス制御部１０４、２０４は、対象１０１、２０１へのアクセスの可否を制御する。

【００２９】配布経路情報蓄積部１０５は、対象アクセス権を当該アクセス権を主体から主体へ順次配布した配布経路情報を格納する。配布経路情報保持部２０６は、配布経路情報蓄積部１０５から読み出され、配布経路情報配布部１２０により配布された情報を、自身の所有する対象あるいは、自身の所有する対象に付随する要素として保存する。

【００３０】アクセス要求部２０７は、配布経路情報で表現された情報を取得した主体（コンピュータＢ）が当該情報を伴い、当該配布経路情報が表現するアクセス権の権限対象である対象へのアクセスを当該対象１０１に付随するアクセス制御部１０４に要求する。アクセス権配布監視部１０８は、アクセス要求部２０７によるアクセス要求に対し、配布経路情報で表現された当該情報を、当該主体（コンピュータＢ）が得るに至るまで、配布経路情報の付与及び配布経路情報の追加、即ち、アクセス権の配布行為が適切に行われたかを確認する。

【００３１】次に、上記の構成における動作を説明する。図４は、本発明の資源アクセス制御動作を示すシーケンスチャートである。

ステップ１０１）　少なくとも１つの主体のコンピュータを経由して、経路情報が主体Ｂに関係するコンピュータＢに配布される。

ステップ１０２）　コンピュータＢにおいて、当該経路情報を取得すると、アクセス権をコンピュータＢからコンピュータＣに配布する処理を行う。このとき、経路情報の取得元情報を経路情報に追加し、主体Ｂに付随する対象として保存する。さらに、アクセス制御情報保部のアクセス制御情報を更新し、経路情報をコンピュータＣに取得可能な状態にする。

【００３２】ステップ１０３）　ステップ１０２で更新された経路情報を主体Ｃに関係するコンピュータＣに配布する。

ステップ１０４）　コンピュータＣでは、当該経路情報を取得すると、アクセス権をコンピュータＤに配布する処理を行う。このとき、経路情報の取得元情報を経路情報に追加し、主体Ｃに付随する対象として保存する。さらに、アクセス制御情報保部のアクセス制御情報を更新し、経路情報をコンピュータＤに取得可能にする。

【００３３】ステップ１０５）　ステップ１０４で更新された経路情報を主体Ｄに関係するコンピュータＤに配布する。

ステップ１０６）　コンピュータＤは、配布権に対応する対象を持つ主体に関係するコンピュータＡに対して、経路情報を伴ったアクセス要求を発行する。

ステップ１０７）　これにより、コンピュータＡでは、配布経路を確認する。確認の方法としては、コンピュータＢ、及びコンピュータＣに対して、経路情報を持っているか、否か、及び経路情報へのアクセス権の有無を確認することにより行う。なお、同図の例では、コンピュータＡが、コンピュータＢ，Ｃに経路情報を配布しているため２回の確認処理を行う例を示しているが、ｎ台のコンピュータに対して配布する場合には、ｎ回の確認処理を行うものとする。

【００３４】ステップ１０８）　ステップ１０７における確認処理において、コンピュータＤからのアクセスを許可するか否かを判定する。

ステップ１０９）　アクセスを許可できる場合には、当該コンピュータＡの対象からアクセス要求されている資源を読み出して、アクセス要求元のコンピュータＤに提供する。

【００３５】次に、アクセス権の配布許諾要求及び、許諾の処理について説明する。図５は、本発明の資源アクセス制御システムの構成図（その２）である。同図に示す構成は、前述の図３の構成において、コンピュータＡに配布許諾確認部１０９とアクセス被配布主体保持部１１０が付加された構成である。配布許諾確認部１０９は、アクセス権の配布に際して、アクセス権の権限対象である対象に付随するアクセス制御部１０４に当該アクセス権配布を報告し、配布の許諾を求める。

【００３６】被配布主体保持部１１０は、配布許諾確認部１０９により報告されたアクセス権被配布主体一覧を保持する。これにより、アクセス制御部１０４は、被配布主体保持部１１０に蓄積された主体一覧により、アクセス権の権限対象である対象の所有主体がアクセス権が配布された主体の範囲を把握し、コンピュータＢのアクセス要求部２０７からのアクセス要求があると、要求主体（コンピュータＢ）が被配布主体保持部１１０に登録されている場合には、アクセス許諾を行う。

【００３７】また、主体Ａにおいて、被配布主体保持部１１０の内容（被配布主体一覧）を任意に更新することにより、アクセス権の権限対象である対象の所有主体が他のアクセス権限配布状況に関係なく、任意の主体へのアクセスを拒否することが可能となる。図６は、本発明の資源アクセス制御動作を示すシーケンスチャート（アクセス許諾）を示す。

【００３８】ステップ２０１）　主体Ｂに関係するコンピュータＢは、少なくとも１つの他の主体を経由した経路情報が配布される。

ステップ２０２）　コンピュータＢは、アクセス権をＣに配布する処理を行う。経路情報取得元情報を、経路情報に追加し、主体Ｂに付随する対象として保存する。さらに、アクセス制御情報を更新し、経路情報をＣに取得可能にすることにより、コンピュータＢからコンピュータＣに経路情報を配布する。また、コンピュータＢは、配布アクセス権に対応する対象を持つ主体に関係するコンピュータＡに対してアクセス権がコンピュータＢからコンピュータＣに配布したことを報告する。これにより、コンピュータＡは、配布先リストを更新する。

【００３９】ステップ２０３）　コンピュータＣは、アクセス権をＤに配布する処理を行う。経路情報取得元情報を、経路情報に追加し、主体Ｃに付随する対象として保存する。さらに、アクセス制御情報を更新し、経路情報をＤに取得可能にすることにより、コンピュータＣからコンピュータＤに経路情報を配布する。また、コンピュータＣは、コンピュータＡに対してアクセス権がコンピュータＣからコンピュータＤに配布したことを報告する。これにより、コンピュータＡは、配布先リストを更新する。

【００４０】ステップ２０４）　ここで、コンピュータＤから経路情報を伴ったアクセス要求がコンピュータＡに対して発行される。

ステップ２０５）　コンピュータＡは、被配布主体保持部１１０に蓄積された主体一覧により、アクセス権が配布された主体Ｄの範囲を把握し、コンピュータ要求主体（コンピュータＤ）が被配布主体保持部１１０に登録されているか否かを判定する。

【００４１】ステップ２０６）　登録されている場合には、アクセス可と判定する。

ステップ２０７）　アクセス可となった場合には、コンピュータＤにアクセス要求対象の資源を提供する。

【００４２】

【実施例】［第１の実施例］最初に、第１の実施例として、経路情報の配布について説明する。図７は、本発明の第１の実施例の動作を説明するための図である。同図に示すシステムにおけるコンピュータＫ＋１（５００）は、Kerberos認証方式（米国マサチューセッツ工科大学を中心に開発されたオープンネットワークを対象とした認証方式）を用いて、主体識別チケット発行部５１０による主体の認証と、当該主体識別チケット発行部５１０により交付される主体識別チケット５２０により主体Ｋ０，主体Ｋ１，…，主体Ｋ，主体Ｋ＋１を一意に識別する。

【００４３】主体がアクセスする対象Ｒ（０）、対象Ｒ（１）、…、対象Ｒ（Ｋ）、対象Ｒ（Ｋ＋１）を対象の保存されているコンピュータの識別子であるコンピュータＫ０、コンピュータＫ１、…、コンピュータＫ－１、コンピュータＫと各々のコンピュータ上で当該対象を区別するローカルな識別子を組み合わせることにより、ネットワーク上で一意に識別する対象識別部（図示せず）を有するコンピュータ１００、２００、３００、４００を、通信回線で相互接続したコンピュータネットワークで、全対象を所有者である主体毎に管理単位として分類し、各々の管理単位毎のアクセス制御リストであるＫ０のアクセス制御リスト１３０、Ｋ１のアクセス制御リスト２３０、…、Ｋのアクセス制御リスト４３０と、各々の管理単位毎のアクセス制御モニタであるＫ０のアクセス制御モニタ１４０、Ｋ１のアクセス制御モニタ２４０、…、Ｋ－１のアクセス制御モニタ３４０、Ｋのアクセス制御モニタ４４０を配置する。

【００４４】ここで、アクセス権の各々の配布行為に伴い、生成される主体Ｋ１の配布経路情報２５０、Ｋの配布経路情報４５０、Ｋ＋１の配布経路情報５５０を用いて、主体識別チケット５２０を伴い、配布経路情報５５０によりアクセス権が配布されている主体Ｋ０の対象Ｒ（０）に付随するＫ０のアクセス制御モニタ１４０へのアクセス要求を発行する。

【００４５】これにより、主体Ｋ０のアクセス制御モニタ１４０は、アクセス権配布経路確認処理を行う。次に、アクセス権の配布及びアクセス権配布経路の確認動作を説明する。アクセス権の配布対象となる主体Ｋ０の

所有する対象Ｒ（０）として識別される文書のアクセス権を、主体Ｋ１、主体Ｋ２、…、主体Ｋ－２、主体Ｋ－１経由で配布された主体Ｋが、新たに主体Ｋ＋１へ対象Ｒ（０）へのアクセス権を配布するには、主体Ｋ０から主体Ｋ－１へアクセス権が配布されてきた経路を表す配布経路情報Ｋを、主体Ｋの対象Ｒ（Ｋ）として保存し、対象Ｒ（Ｋ）へのアクセス権を主体Ｋのアクセス制御リスト４３０を変更することにより、主体Ｋ＋１にアクセス権を与える。

【００４６】主体Ｋ＋１は、対象Ｒ（Ｋ）にアクセスし、主体Ｋ０から主体Ｋへアクセス権が配布されてきた経路を表す配布経路情報Ｋを取得し、配布経路情報Ｋを主体Ｋの対象Ｒ（Ｋ）から取得したものであることを表現するエントリ（Ｋ，Ｒ（Ｋ））を配布経路情報Ｋ（４５０）の最後尾に付加し、Ｋ０からＫへアクセス権が配布されてきた経路を表す配布経路情報Ｋ＋１（５５０）とし、後述する手順により、本来アクセス権の配布対象である主体Ｋ０の対象Ｒ（０）へのアクセス権として利用する。

【００４７】第三者への再配布をする場合は、配布経路情報Ｋ＋１（５５０）を主体Ｋ＋１（５００）の対象Ｒ（Ｋ＋１）として保存する。配布されたアクセス権の監査は以下の手順で実施する。主体Ｋ＋１（５００）が主体Ｋ０（１００）の対象Ｒ（０）へアクセスする際には、主体Ｋ０から主体Ｋへのアクセス権配布を表現する配布経路情報Ｋ＋１（５５０）を伴って、主体Ｋ０（１００）のアクセス制御モニタ１４０に要求する。主体Ｋ０（１００）のアクセス制御モニタ１４０は、配布経路情報Ｋ＋１（５５０）に従って、Ｋのアクセス制御モニタ４４０、Ｋ－１のアクセス制御モニタ３４０、…、Ｋ１のアクセス制御モニタ２４０に順次確認する。

【００４８】具体的には、確認動作（Ｋ）で主体Ｋ（４００）のアクセス制御モニタ４４０に主体Ｋの対象Ｒ（Ｋ）が主体Ｋ０から主体Ｋ－１への配布経路に一致し、主体Ｋ＋１（５００）にアクセス権が与えられていることを確認する。次に、確認動作（Ｋ－１）で主体Ｋ－１のアクセス制御モニタ３４０に主体Ｋの対象Ｒ（Ｋ－１）が主体Ｋ０から主体Ｋ－２への配布経路に一致し、主体Ｋにアクセス権が与えられていることを確認する。

【００４９】以下、アクセス権の配布経路におけるアクセス制御モニタに順次確認していき、最終的には、確認動作（１）で、Ｋ１のアクセス制御モニタ２４０に主体Ｋ１の対象Ｒ（１）が主体Ｋ０の対象Ｒ（０）を指示し、主体Ｋ２にアクセス権が与えられていることを確認する。さらに、確認動作（０）でＫ０のアクセス制御モニタ１４０に主体Ｋ０の対象Ｒ（０）が主体Ｋ１にアクセス権が与えられていることを確認する。最終的に、全配布経路が確認されたら、そのアクセス権は正当なものと判断し、主体Ｋ０のアクセス制御モニタ１４０にはアクセスを許可する。

【００５０】［第２の実施例］次に、第２の実施例としてアクセス要求に対するアクセス許諾について説明する。図８は、本発明の第２の実施例の動作を説明するための図である。同図では、アクセス権限の配布動作を示す配布（０）、配布（１）、…、配布（Ｋ－１）、配布（Ｋ）に対応する報告動作を示す報告（０）、報告（１）、…、報告（Ｋ－１）、報告（Ｋ）を行うための機能及び配布先管理リスト１６０を有する。

【００５１】実際のアクセス権の配布及び報告は、以下の手順で行われる。アクセス権を主体Ｋ０～Ｋ１へ配布する配布動作（０）に際しては、報告動作（０）により配布の許諾が行われ、配布先管理リスト１６０に配布先であるＫ１が追加される。以下、配布動作（１）、…、配布動作（Ｋ）に対しても同様の報告と登録が行われる。

【００５２】Ｋ（０）のアクセス制御モニタ１４０は、アクセス要求主体がアクセス権限配布先管理リスト１６０に登録されていることを、アクセス許可条件に加えて判定し、アクセスを許可する。これにより、主体Ｋ０は、配布先管理リスト１６０により常時アクセス権保持者を確認できると同時に、配布先管理リスト１６０から任意の主体を削除することにより、前述の第１の実施例によるアクセス権配布によるアクセス許諾とは独立に、主体Ｋ０による任意の主体に対するアクセス拒否を可能とする。

【００５３】また、上記の実施例は、前述の図３及び図５の構成及び、図４及び図６の動作に基づいて説明しているが、これらの構成要件及び動作をプログラムとして構築し、ネットワーク上の主体のコンピュータのディスク装置や、フロッピーディスクやＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際に、インストールすることにより容易に本発明を実現できる。

【００５４】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００５５】

【発明の効果】上述のように、本発明によれば、アクセス権の配布を可能とすると共に、アクセス権の配布行為がアクセス権を表現する配布経路情報という実存の情報の授受で行われるため、監査が容易であるだけでなく、アクセス権の行使に際して、アクセス権の配布に関連した全ての主体に確認するため、アクセス権の剥奪制御が容易に実現できる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

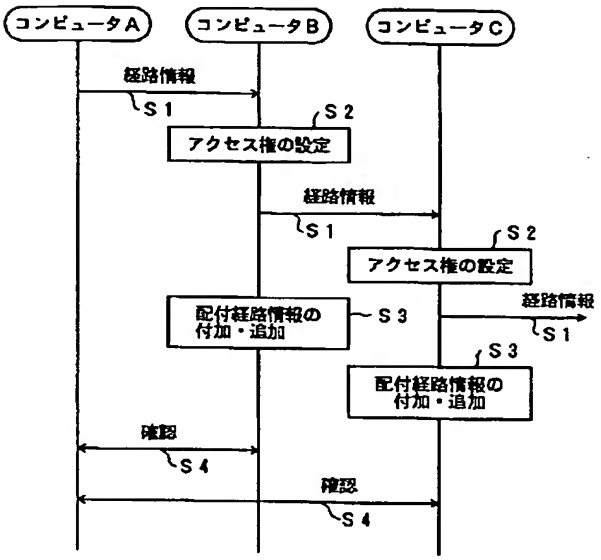
【図３】本発明の資源アクセス制御システムの構成図（その１）である。

【図４】本発明の資源アクセス制御動作を示すシーケン

スチャート（経路情報配布）である。
【図５】本発明の資源アクセス制御システムの構成図（その２）である。
【図６】本発明の資源アクセス制御動作を示すシーケンスチャート（アクセス許諾）である。
【図７】本発明の第１の実施例の動作を説明するための図である。
【図８】本発明の第２の実施例の動作を説明するための図である。
【図９】従来の一般的アクセス制御モデルである。
【図１０】従来の三つ組表を用いるアクセス制御方式（第１の方式）である。
【図１１】従来の資格を用いるアクセス制御方式（第２の方式）である。
【図１２】従来のアクセス制御リストを用いるアクセス制御方式（第３の方式）である。
【図１３】従来のアクセス制御マトリクスに対するアクセス制御モデルである。
【図１４】従来の鍵と錠を用いるアクセス制御方式（第４の方式）である。
【図１５】従来の配布、被配布の関係を保持するアクセス制御情報の実現方式（第５の方式）である。
【図１６】従来の配布、被配布の関係を保持しないアクセス制御情報の実現方式（第６の方式）である。
【符号の説明】
１０　経路情報
２０　経路情報配布手段
３０　アクセス権設定手段
４０　更新手段
５０　確認手段
１００　コンピュータＫ０
１０１　対象（資源）
１０２、２０２　対象識別部
１０３、２０３　アクセス制御情報保持部
１０４、２０４　アクセス制御部
１０５　配布経路情報蓄積部
１０８　アクセス権配布監視部
１０９　配布先許諾確認部
１１０　アクセス被配布主体保持部
１１１、２１１　対象アクセス部
１２０　配布経路情報配布部
１３０　Ｋ０のアクセス制御リスト
１４０　Ｋ０のアクセス制御モニタ
１６０　配布先管理リスト
１９０、２９０　主体識別部
２００　コンピュータＫ１
２３０　配布経路情報Ｋ１
２４０　Ｋ１のアクセス制御モニタ
２５０　配布経路情報Ｋ１
３００　コンピュータＫ－１
３４０　Ｋ－１のアクセス制御モニタ
４００　コンピュータＫ
４３０　Ｋのアクセス制御リスト
４４０　Ｋのアクセス制御モニタ
４５０　配布経路情報Ｋ
５００　コンピュータＫ＋１
５１０　主体識別チケット発行部
５２０　主体識別チケットＫ＋１
５５０　配布経路情報Ｋ＋１
２０６　配布経路情報保持部
２０７　アクセス要求部
２２０　配布経路情報取得部

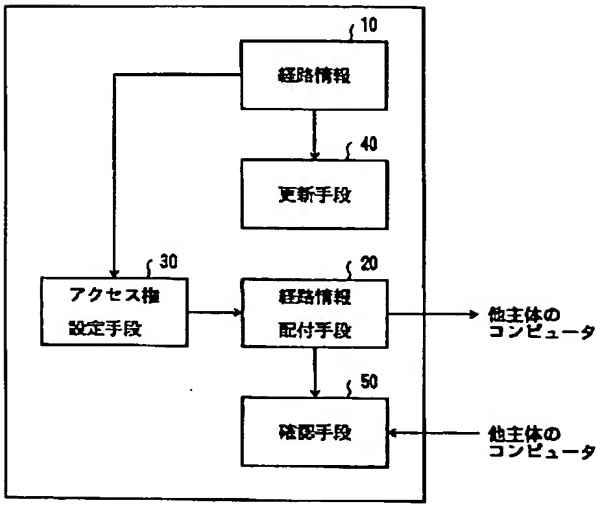
【図１】

本発明の原理を説明するための図



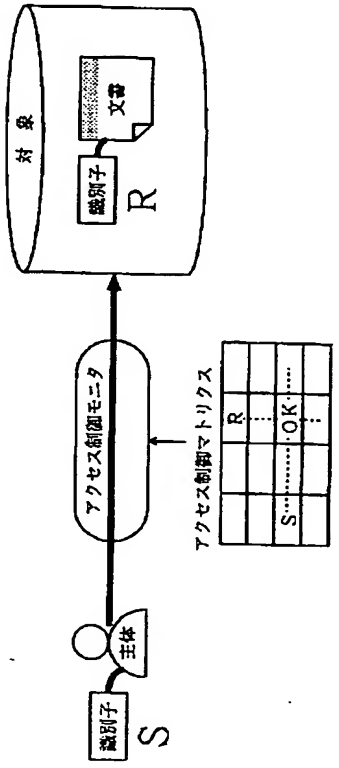
【図２】

本発明の原理構成図



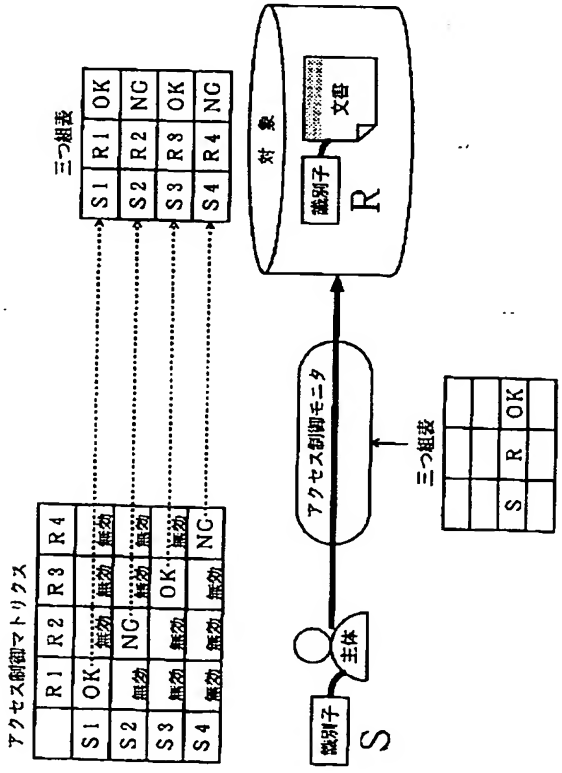
【図９】

従来の一般的アクセス制御モデル



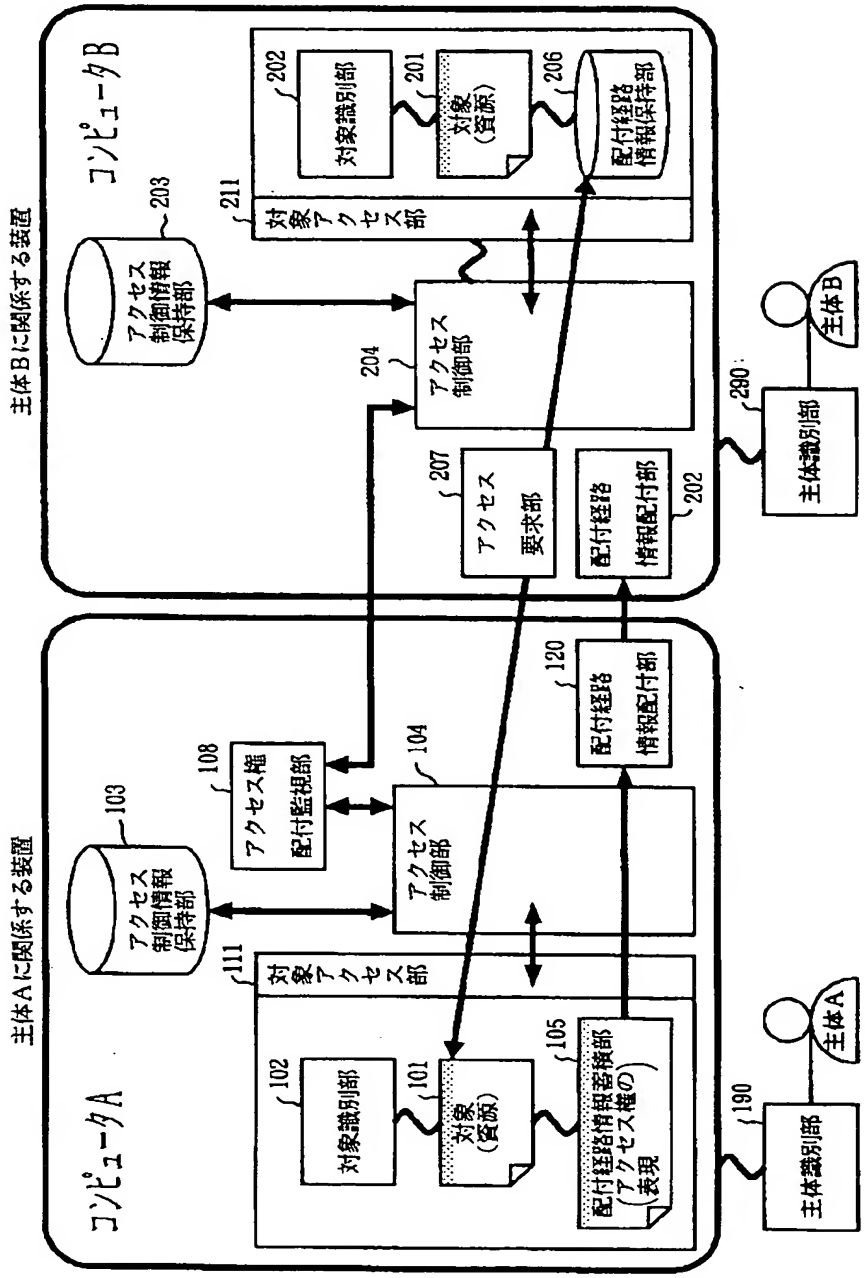
【図１０】

従来の三つ組表を用いるアクセス制御方式（第１の方式）



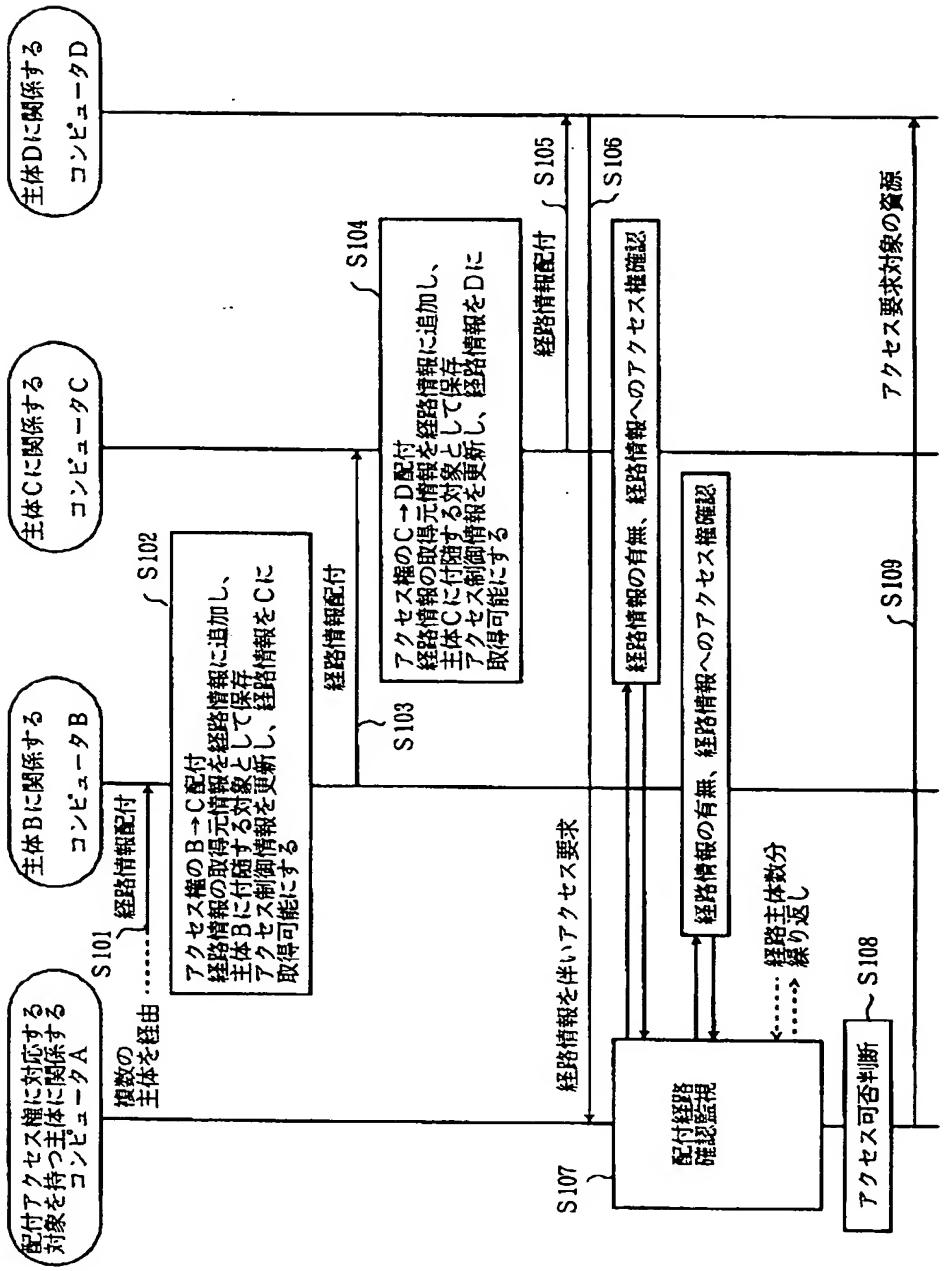
【図３】

本発明の資源アクセス制御システムの構成図（その１）



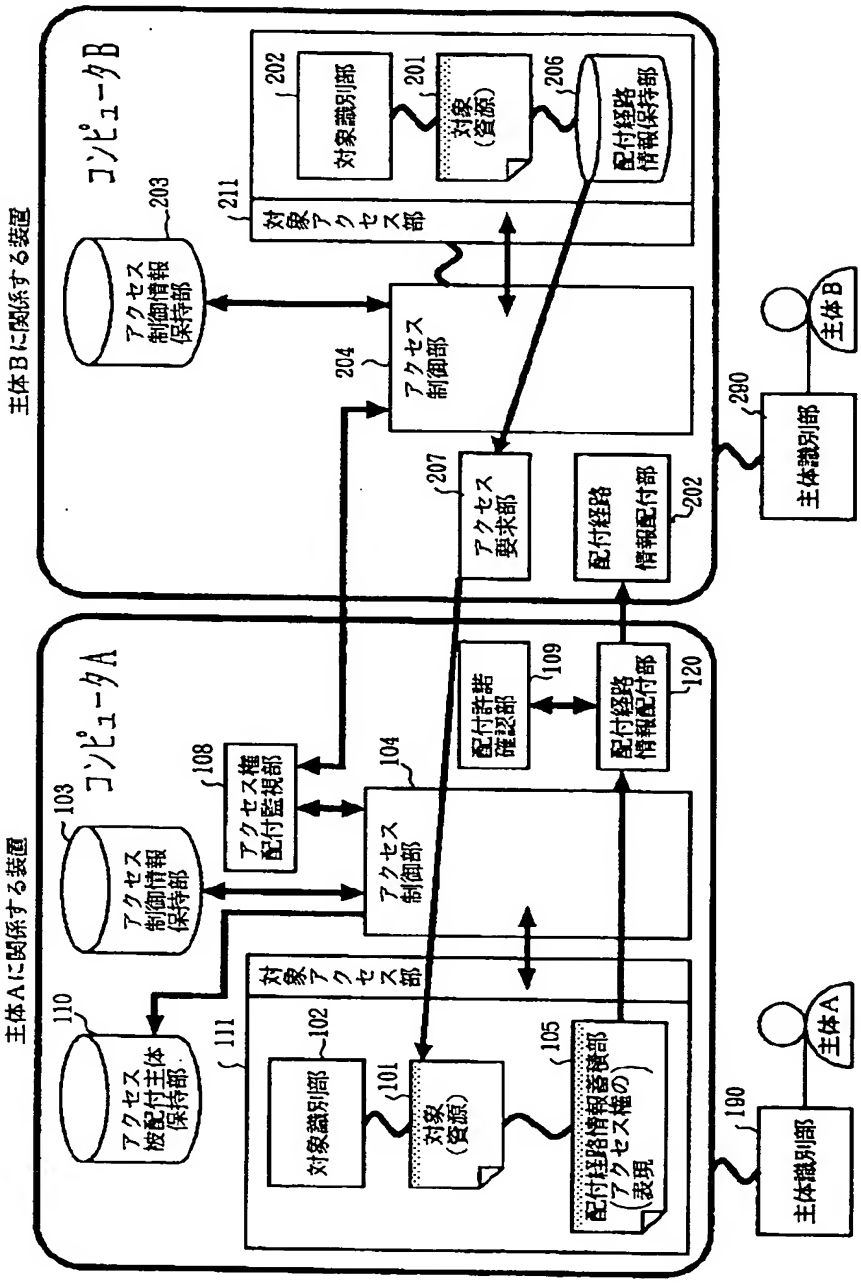
【図４】

本発明の資源アクセス制御動作を示す
シーケンスチャート（経路情報配付）



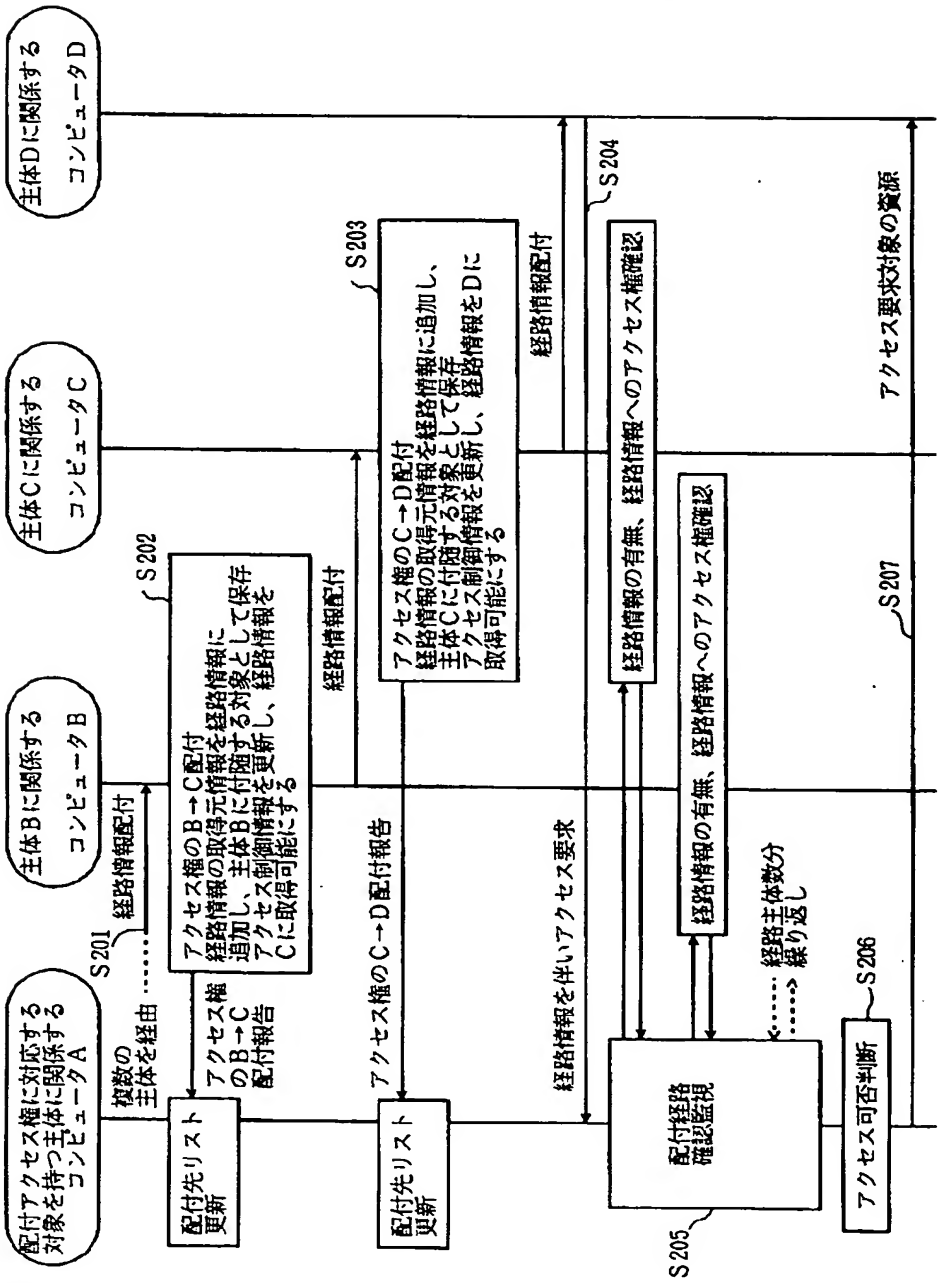
【図５】

本発明の資源アクセス制御システムの構成図（その２）



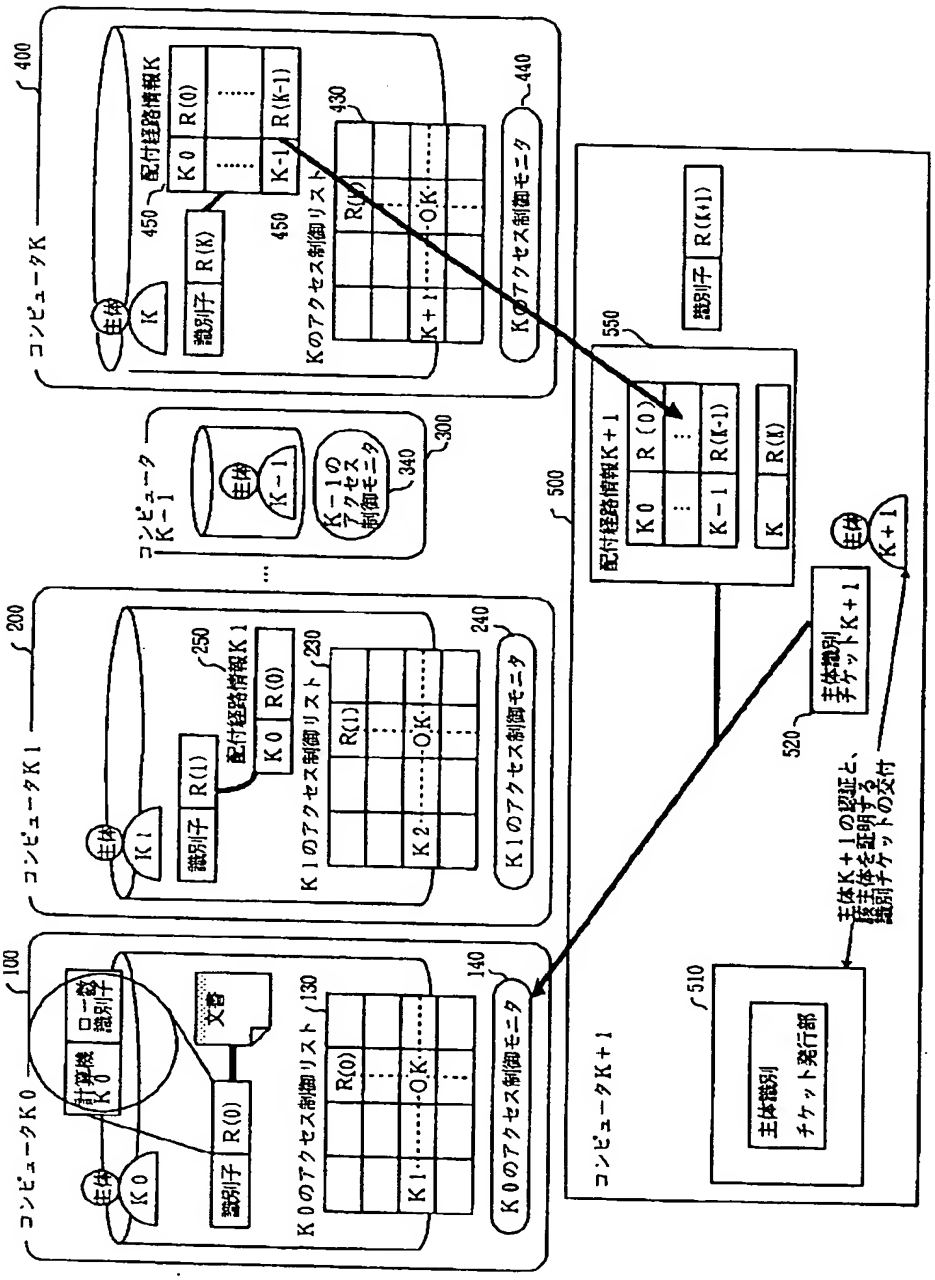
【図６】

本発明の資源アクセス制御動作を示す
シーケンスチャート（アクセス許諾）



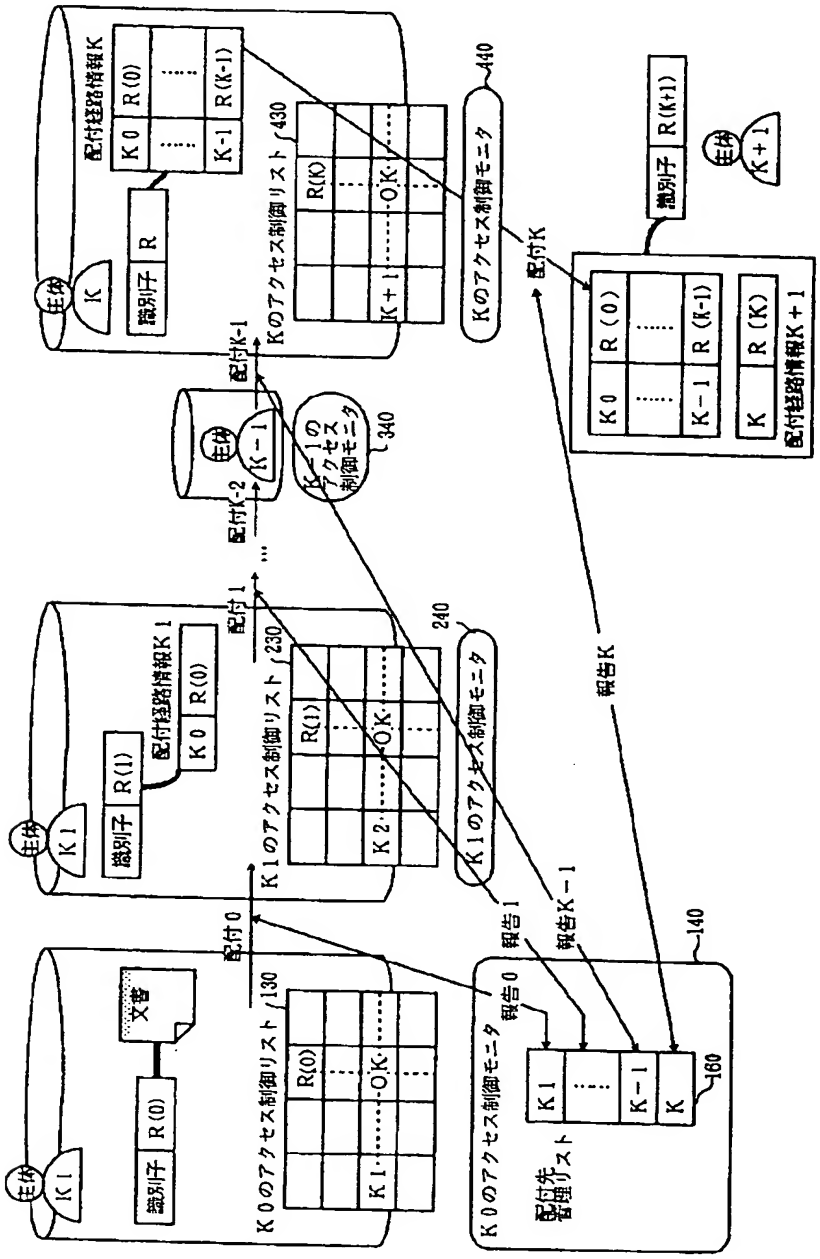
【図７】

本発明の第１の実施例の動作を説明するための図



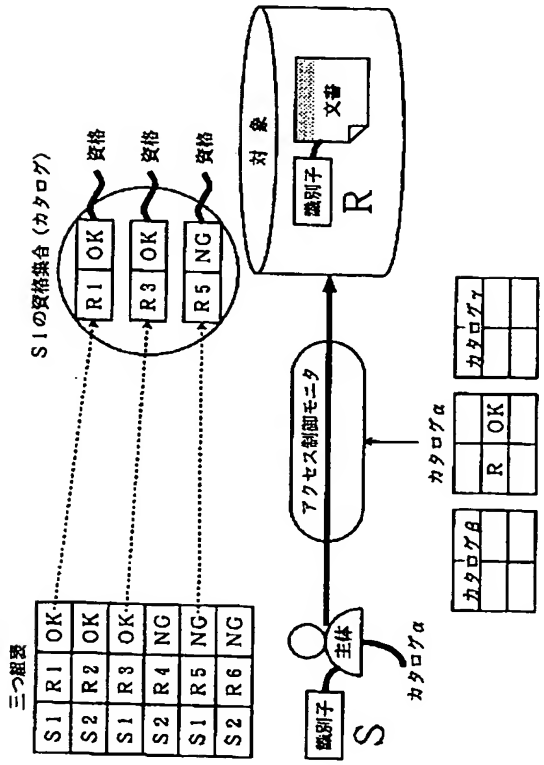
【図８】

本発明の第２の実施例の動作を説明するための図



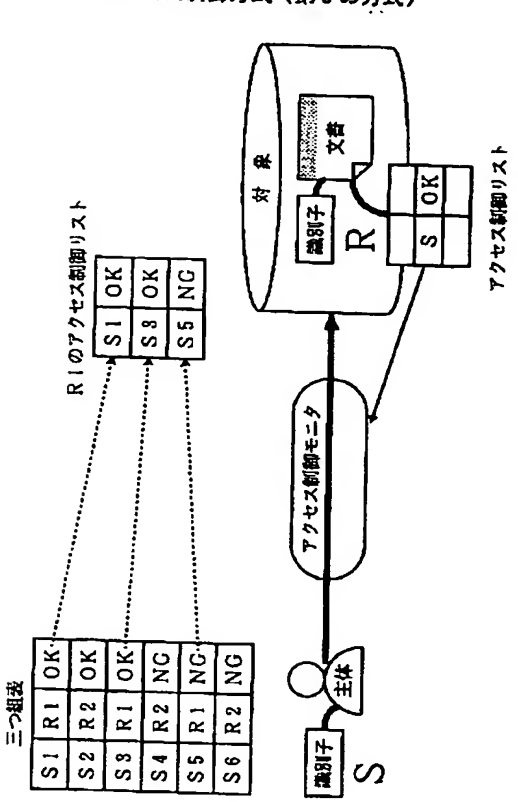
【図１１】

従来の資格を用いるアクセス制御方式（第２の方式）



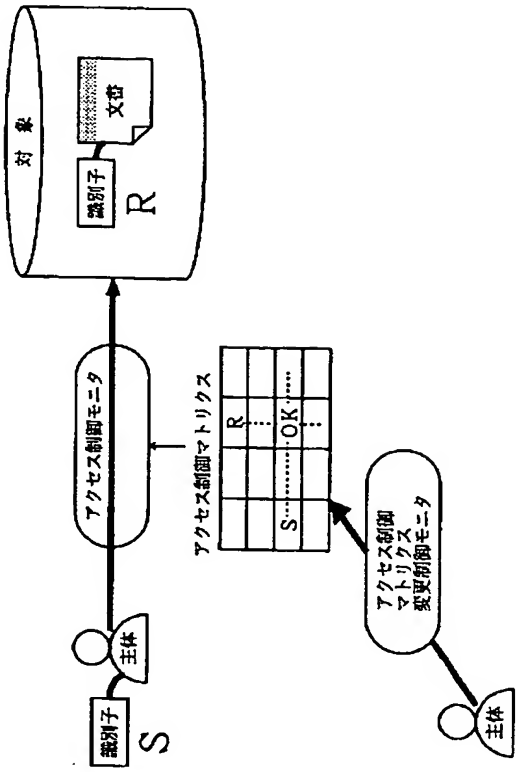
【図１２】

従来のアクセス制御リストを用いる
アクセス制御方式（第３の方式）



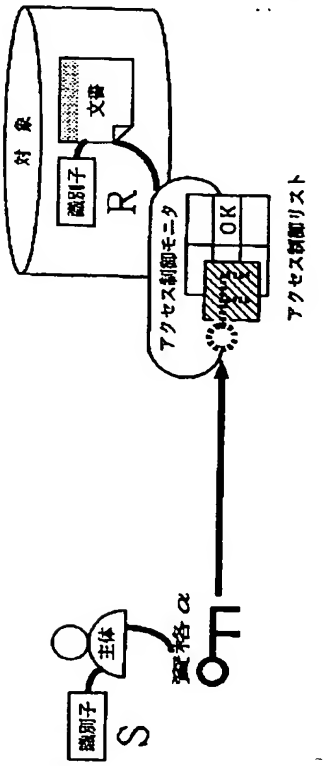
【図１３】

従来のアクセス制御マトリクスに対するアクセス制御モデル



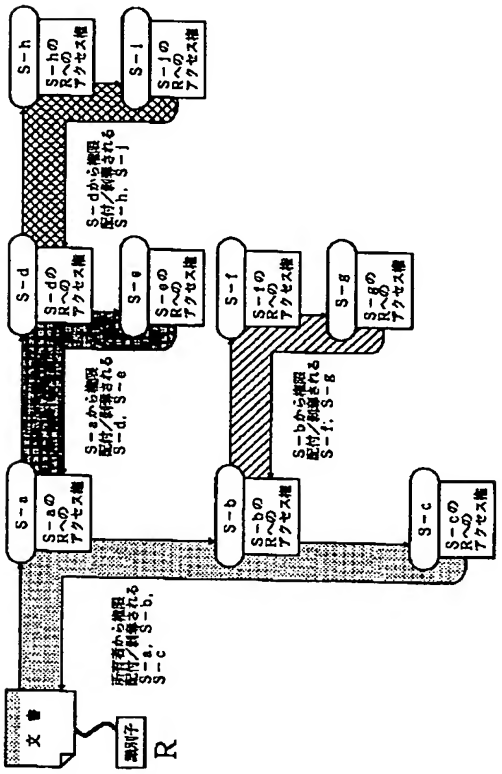
【図１４】

従来の鍵と錠を用いるアクセス制御方式（第４の方式）



【図１５】

従来の配付、被配付の関係を保持する
アクセス制御情報の実現方式（第５の方式）



【図１６】

従来の配付、被配付の関係を保持しない
アクセス制御情報の実現方式（第６の方式）